Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of controlling security of data in a storage system having a local disk system and a remote disk system that are coupled to at least one host computer, the method comprising:

in the local disk system coupled to a first host computer, the local disk system having first and second volumes of storage, the first and second volumes associated with first and second encryption keys, respectively:

when a write of data is to be made to the first volume of the local disk system, retrieving the first encryption key;

encrypting the data using the first key, the encrypting being performed by the local disk system;

transferring the encrypted data to the remote disk system via a first communication link; then

in the remote disk system:

determining whether the data is to be stored in an encrypted form or a decrypted form, the determining being performed by the remote disk system;

determining an address for storage of the data in the remote disk system;

if the data is to be stored in a decrypted form, decrypting and writing the data in the remote disk system;

if the data is to be stored in an encrypted form, writing the data in the remote disk system without decrypting the data; and

notifying the local disk system via the first communication link that the step of writing the data is complete,

wherein the local disk system is coupled to the first host computer via a second communication link to allow the first host computer to access data stored in the local disk system, the first and second communication links being different,

wherein the remote disk system includes third and fourth volumes corresponding to the first and second volumes, respectively.

2. (Previously Presented) A method of controlling security of data in a storage system having a local disk system and a remote disk system that are coupled to at least one host computer, the method comprising:

in the local disk system coupled to a first host computer:

when a write of data is to be made to the local disk system, a previously stored encryption key;

encrypting the data using the key, the encrypting being performed by the local disk system;

transferring the encrypted data to the remote disk system via a first communication link; then

in the remote disk system:

determining whether the data is to be stored in an encrypted form, the determining being performed by the remote disk system;

determining an address for storage of the data in the remote disk system;

if the data is to be stored in a decrypted form, decrypting and writing the data in the remote disk system;

if the data is to be stored in an encrypted form, writing the data in the remote disk system without decrypting the data; and

notifying the local disk system via the first communication link that the step of writing the data is complete,

wherein the local disk system is coupled to the first host computer via a second communication link to allow the first host computer to access data stored in the local disk system, the first and second communication links being different,

wherein the method further comprises maintaining an encryption control table on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local and the remote disk system,

wherein the data transfer between the local disk system and the remote disk system occurs via a communication link that couples the local disk system to the remote disk system, so that the local disk system may send the data to the remote disk system without direct involvement from the host computer,

wherein the list of encryption keys includes the first and second keys, the first key being assigned to a first set of volumes in the local disk system, and the second key being assigned to a second set of volumes in the local disk system, each of the first and second set of volumes including one or more volumes,

wherein the retrieving step includes accessing the encryption control table to obtain an appropriate encryption key, where the data are encrypted using the first key if the data to be transferred to the remote disk system are associated with the first set of volumes and encrypted using the second key if the data to be transferred to the remote disk system are associated with the second set of volumes,

wherein the remote disk system is coupled to a second host computer.

3. (Original) A method as in claim 2 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local disk system.

4. (Original) A method as in claim 2 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote disk system.

5. (Original) A method as in claim 3 wherein the encryption key is applicable to less than all of the storage on the local disk system.

6. (Original) A method as in claim 4 wherein the encryption key is applicable to less than all of the storage on the remote disk system.

7. (Original) A method as in claim 3 wherein the encryption key is applicable to at least one disk on the local disk system.

8. (Original) A method as in claim 7 wherein the encryption key is applicable to at least one disk on the remote disk system.

9. (Previously Presented) A method for changing an encryption key while operating a storage system having a local disk system and a remote disk system comprising:

storing an encryption key in a memory in the local disk system;

transmitting the encryption key to the remote disk system and storing it in a memory there via a first communication link coupling the local and remote disk systems;

in the local disk system, determining a boundary for use of the encryption key by the local disk system;

in the remote disk system, receiving the boundary from the local disk system by the remote disk system;

in both the local and the remote disk systems, determining a relationship of present operations to the boundary by each of the local and remote disk systems;

in both the local and the remote disk systems, waiting for the boundary and then changing the encryption key for data stored thereafter by each of the local and remote disk systems,

wherein the local disk system is coupled to a first host computer via a second communication link that is different than the first communication link.

10. (Original) A method as in claim 9 wherein operations before the boundary are performed using a first encryption key and operations after the boundary are performed using a second encryption key.

11. (Original) A method as in claim 9 wherein the boundary is defined by counting input/output operations and using the count to define the boundary.

12. (Canceled)

13. (Previously Presented) A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

maintaining a control table in each of the local disk system and the remote disk system;

determining a boundary in the local disk system where encryption is to be switched to an opposite state, the determining performed by the local disk system;

in the remote disk system, receiving a corresponding boundary from the remote disk system;

in both the local and the remote disk system, determining a relationship of present operations to the boundary;

in both the local and the remote disk system waiting for the boundary, and then changing the encryption to the opposite state,

wherein the local disk system is coupled to a first host computer via a first communication link, and the remote disk system is coupled to a second host computer via a second communication link, the local disk system and the remote disk system being coupled to each other via a third communication link, the third communication link being different than the first or second communication link.

14. (Original) A method as in claim 13 wherein operations before the boundary are either encrypted or not encrypted, and operations performed after the boundary are either not encrypted or encrypted oppositely to those operations performed before the boundary.

15. (Original) A method as in claim 14 wherein the boundary is defined by counting input/output operations and using the count to define the boundary.

16. (Previously Presented) A method of controlling encryption in a storage system having a local disk system and a remote disk system comprising:

storing first and second encryption keys in a memory in the local disk system that is coupled to a host computer via a first communication link, the first and second encryption keys assigned to first and second volumes of the local disk system, respectively;

transmitting via a second communication link the first and second encryption key to the remote disk system and storing it in a memory there, the remote disk system including third and fourth volumes corresponding to the first and second volume, respectively;

splitting the local disk system from the remote disk system to allow them to operate independently, wherein the splitting is performed according to a first command issued by the local or remote disk system;

switching encryption to an opposite state from a previous state after splitting the local disk system and remote disk system; and

re-synchronizing the local disk system and the remote disk system, wherein the re-synchronizing is performed according to a second command issued by the local or remote disk system, the first and second communication links being different.

17. (Previously Presented) A storage system comprising:

a local disk system including a plurality of volumes of media for storing data, said local disk system being coupled to a host computer via a first communication link to enable the host computer to access said volumes, the plurality of volumes in the local disk system including first and second volumes that are associated with first and second encryption keys, respectively;

a remote disk system including a plurality of volumes of media for storing data; and

a second communications link coupling the local disk system to the remote disk system,

wherein the local disk system determines whether encryption is to be employed in the data associated with the first volume in the local disk system, and if so, the local disk system encrypts the data to be transferred to the remote disk system using the first key, and

wherein the remote disk system determines whether to store the data in either encrypted form or unencrypted form and stores the data in that form in the remote disk system, and notifies the local disk system that the data has been stored via the second communication link,

wherein the first and second communication links are different.

18. (Original) A system as in claim 17 further comprising an encryption control table stored on the local disk system, the encryption control table including a list of encryption keys for selected volumes of the local system and the remote system.

19. (Original) A system as in claim 18 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the local system.

20. (Original) A system as in claim 19 wherein the list of encryption keys further includes information relating to the use and non-use of encryption on the remote system.

21. (Original) A system as in claim 20 wherein the encryption key is applicable to less than all of the storage on the local system.

22. (Original) A system as in claim 21 wherein the encryption key is applicable to less than all of the storage on the remote system.

23. (Canceled).

24. (Canceled).

25. (Canceled).

26. (Previously Presented) A system for controlling encryption in a storage system having a local disk system and a remote disk system comprising:

a local memory in the local disk system for storing a first encryption key assigned to a first volume in the local disk system and a second encryption key assigned to a second volume in the local disk system;

a first communications link for transmitting the first and second encryption keys to the remote disk system and storing the first and second encryption keys in a remote memory of the remote disk system;

a first computer program for splitting the local disk system from the remote disk system to allow them to operate independently;

a switch for changing encryption to an opposite state from a previous state after splitting in the local disk system and remote disk system; and

a second computer program for re-synchronizing the local disk system and the remote disk system,

wherein the local disk system is coupled to a host computer via a second communication link that is different than the first communication link,

wherein the local disk system is configured to execute the first computer program or the second computer program, or both,

wherein the local disk system is configured to encrypt data to be transferred to the remote disk system using the encryption key that is stored in the local memory of the local disk system.

27. (Previously Presented) A method of controlling security of data in a storage system having a local disk system and a remote disk system comprising:

in the local disk system, the local disk system including first and second volumes that are assigned first and second encryption keys, respectively:

receiving a data update request from a host computer connected to the local disk system wherein said data update request includes a location of the first volume of the local disk system, the host computer being connected to the local disk via a first communication link;

encrypting the data associated with the first volume of the local disk system using the first key by the local disk system;

transferring the encrypted data to the remote disk system via a second communication link by the local disk system; then

in the remote disk system:

decrypting the data using the first key by the remote disk system; and

writing the decrypted data into a third volume of the remote disk system by the remote disk system,

wherein the first and second communication links are different.

28. (Canceled)

29. (Canceled)

30. (Previously Presented) A storage system comprising:

a local disk system including first and second storage volumes for storing data, the first and second volumes being assigned with first and second encryption keys, respectively, wherein the local disk system is connected to a host computer via a first communication link;

a remote disk system including third and fourth storage volumes, respectively, for storing data;

a second communications link coupling the local disk system to the remote disk system, the first and second communication links being different,

wherein the local disk system retrieves selected data from the first volume in the local disk system, encrypts the selected data using the first encryption key, and transmits the encrypted data to the remote disk system, and

wherein the remote disk system decrypts the encrypted data received from the local disk system via the second communications link and stores the data in unencrypted form in the third volume in the remote disk system.

31. (Previously Presented) A system as in claim 30 further comprising an encryption control table stored on the local disk system, the encryption control table including the firs and second keys.

32. (Previously Presented) A method of controlling security of data in a disk system coupled to a host computer and a remote storage system, the method comprising:

at the disk system, receiving data to be stored from the host computer via a first communication link, so that the data can be stored in a given area in the disk system, the disk system including first and second volume that are assigned first and second encryption keys, respectively,;

encrypting the data received from the host computer using the first or second key according to the location of the given area, wherein the first key is used if the given area in the first volume and the second key is used if the given area is in the second volume, the encrypting performed by the disk system; and

transferring the encrypted data to the remote storage system via a second communication link by the disk system, so that the remote storage system can store the data therein.

33. (Canceled)

34. (Canceled)